Identification and Authentication

This module describes the concepts of identification andauthentication (I&A). It examines the three approaches to authentication and introduces the concept of trusted path. Selected implementations of I&A mechanisms are described.

Module Learning Objectives

The material presented in this module can be read independently of theother modules. Upon completion of this module, the student should:

1. Understand what I&A is and why it is needed.
2. Understand the TCSEC requirements for I&A.
3. Be familiar with various mechanisms that strengthen the protection provided by I&A mechanisms, such as trusted path.

Overview

The concepts of “identification” and “authentication” are soc losely associated that they are sometimes mistakenly considered to be the same operation. Identification is the first step a user must take in accessing atrusted system. It is the process of identifying the account the user wants to use to access the system. Authentication is the process of proving that the user is theowner of the requested account and has the right to use it. Both identificationand authentication are essential for establishing credible identity; neither mandatory nor discretionary security policies can be properly invokedwithout assurance that a valid user ID has been correctly associated with itsreal user .

The TCSEC requirements for I&A in trusted systems start at C1 byrequiring that users first identify and authenticate themselves to the systembefore being permitted to perform any other action. Authentication data must beprotected from unauthorized access. C2 requires that the TCB must be able to uniquely identify each user, so that individual's can be held accountable for their use of the trusted system. B1 requires that the TCB maintain clearance and authorization data about each user to support the mandatory access control mechanisms required at B1. B2 requires that the TCB provide a trusted communication path between itself and the user for initial login and authentication. Communication via this path is initiated exclusively by the user. B3 requires that the trusted path be available for other security-relevant operations besides login and authentication. The TCSEC requirements have been expanded by later Interpretations.

Authentication

There are three general approaches to authentication. The most common approach is to authenticate a user based on something only the user should know, such as a secret password. Another approach is to authenticate a user based on something the user uniquely possesses, such as a physical card or key. A third approach is to authenticate a user based on something physically unique about the user himself, such as fingerprints. The advantages and disadvantages of these approaches are discussed in detail in [Wood77] and [Carlton88], and are summarized below:

1. Authenticate on something the user alone knows (e.g., passwords)

   Advantages:

   - Easy to use and a familiar technology.
   - Easy and inexpensive to implement and manage.
   - Most common and richest knowledge base on usage and management.

   Disadvantages:

   - Easy for the user to accidentally divulge the authentication data.
   - Does not address the threat of eavesdropping authentication data off an insecure channel.
   - Susceptible to exhaustive search attacks.
   - Authentication data that is hard to guess is hard to remember.

2. Authenticate on something the user uniquely possesses (e.g., physical card, house key)

   Advantages:

   - Loss of object alerts user to possible attack (unlike the loss of a password).
   - Very difficult to spoof without possession of object or accurate duplicate.

   Disadvantages:

   - Must be complex enough to discourage duplication.
   - Potentially high cost for manufacturing and/or distribution.
   - Physical object is too loosely associated with a user -- anyone gaining possession of object will be successfully authenticated if another form of authentication is not also required.

3. Authenticate on something physically unique about the user (e.g., biometric feature such as fingerprint, voice, weight, retina pattern, etc.)

   Advantages:

   - Feature associated directly with user so cannot be transferred and used by other user.
   - Complexity of biometric feature makes it inherently hard to spoof.

   Disadvantages:

   - Must be properly tuned to permit some tolerance to natural variation (e.g., voice change due to a cold) but not be open to mimicking.
   - Generally, to be discriminating, requires expensive scanning equipment.
   - May intrude on individual's privacy.

The most common authentication method is the management of passwords. This system is dependent on how well users keep their password secret(i.e ., by not writing it down or letting others watch as they type it), how well the system keeps the password secret (i.e., by encrypting the password and preventing unauthorized access, and the prevention of eavesdropping), and how hard the password is to guess. Passwords should be of sufficient length and character diversity to minimize the threat of exhaustive search and simple guessing, and should not be biased by easily researched “personal” information (e.g., spouse's name, favorite musician, etc.). A machine generated password is beneficial, but makes it more likely that the user will write the password down on paper, especially in environments with multiple machines and infrequent use. Machine generated passwords should include features that make the generated passwords more memorable, such as making them human pronounceable. Forcing the regular changing of passwords also lessens the threat of password compromise, but increases the likelihood that a password will be written down, rather than memorized. Comprehensive guidelinesfor the creation and management of password authentication is provided in [PASS85].

Password systems are inherently weak in many respects. Foremost is the need to trust users not to disclose their “secret.” Users must be educated of the importance not to choose “easy” passwords or let others use their account. Users must be taught that even if they only use their account for checking public messages and have nothing of value to lose personally if their account is broken into, they have a responsibility to the rest of the system's users to prevent unauthorized access.

I&A's resistance to penetration is strengthened by the adoption of ahybrid approach that combines complementary authentication mechanisms. A common example of this is the pairing of an automated teller machine (ATM) card with its corresponding personal identification number (PIN)so that trust is not placed on one mechanism alone for successful authentication.

A challenge-response one-time password mechanism is a particularly effective hybrid approach that minimizes the disadvantages and maximizes the advantages of two I&A approaches. In this approach the user possesses an electronic device uniquely associated with him/her and a PIN that is usedto activate the device. The device calculates the required response based on a challenge issued by the system being logged into. Only if this one-time response matches the response expected by the system is the authenticationsuccessful.

An example commercial implementation adopted for use by the NCSC's Dockmaster system is the Racal-Guardata Watchword device (developed by Sytek and formerly marketed by them as the PFX A2000 PassPort). This calculator-like device has been evaluated under the NCSC sub-system evaluation program. To be authenticated by Watchword the following steps occur:

- Each user is assigned a Watchword device that is uniquely identified by a secret key and a PIN that is used to activate the Watchword.

- In response to the standard host machine login prompt the user enters a unique identifier, also called a user ID, and a password.
- The host's authentication server checks to see if the user ID is valid for the password entered. Next, the system generates, using the secret key associated with that user, a seven digit challenge and expected response pair not previously used. The challenge is then presented to the user. Even if the user ID/ password pair is not valid, a challenge is still issued but the user will not be authenticated.
- The user enters his/her PIN into his/her Watchword.
- The user enters the host-generated challenge into the Watchword. The Watchword computes a response based on the challenge, the user entered PIN, and the secret key associated with that particular Watchword.
- The user supplies the response generated by the Watchword to the host system, and the host compares the user's response to the response predicted by the authentication server. If the user has entered the correct response, the user is successfully authenticated.

The strength of the Watchword I&A procedure is thus based on the required physical possession of a unique authentication device and the knowledgeof the associated PIN. The information that is transmitted between the user and the host during authentication is never reused, which foils spoofing and eavesdropping/playback attacks. Because the user is permitted to generate responses on demand, the need for synchronization between the user's device and the system is avoided.

Trusted Path

An important consideration in securely performing I&A, particularly forhigh assurance systems, is that not only must the user authenticate himself or herself to the TCB, but the TCB must also effectively authenticate itself to the user. The user must have assurance that he or she is communicating directly with the TCB so as to prevent the possibility that Trojan horse software is spoofing the user into relinquishing secret authentication data. This requirement is referred to as establishing a trusted path, and is usefulnot only for I&A, but also for such security sensitive tasks as changing the current security level or, for administrators, changing security attributes attached to subjects or objects.

The TCSEC requires that a trusted path be used for logging into a system beginning at B2, and at B3 for any action that changes the data base or rules that the TCB uses during checks for security policy violations. Trusted path is generally implemented by sending a break signal that cannot beintercepted or faked by non-TCB software. This signal causes the TCB to grab the terminal away from untrusted software that might be using the terminal. A trusted path implementation is described in [Wisema88].

Relevant Trusted Product Evaluation Questionnaire Questions

2.6 IDENTIFICATION & AUTHENTICATION (I&A)

C1:

1. (a) Does the system require the users to provide identification at the time of login? (b) If yes, what information is requested bythe system?
2. Is there any additional device or physical security required for user identification and authentication (I&A) (e.g., terminalID, passkey, smart card, etc.)?
3. (a) Does the system authenticate this identity at the time oflogin? (b) If yes, what information is requested by the system? (c)How does the system use this information to authenticate the identity?
4. (a) Describe the algorithms used in user authentication. (b) Where in the system are the code and data for authentication (e.g., user/password data base) stored?
5. How are the authentication code and data protected?
6. (a) Does the I&A process associate privileges with the user? Ifso, (b) what and (c) how?

C2:

7. Describe how each user is uniquely identified.

B1:

8. How does the I&A process associate a sensitivity level with the user?

2.13 OTHER ASSURANCES

B2:

9. (a) When (e.g., before user authentication) and (b) how(e.g., by typing a specific control character sequence) can the trusted path be invoked by the user? (c) What TCB elements are involved in establishing the trusted path?
10. How does the TCB ensure that the trusted path is unspoofable?

B3:

12. What security relevant actions are able to be performed under trusted path?
13. Are there other system interfaces which support the same functionality as provided in the trusted path?

Required Readings

TCSEC85 National Computer Security Center, *Department of Defense Trusted Computer Security Evaluation Criteria*, DoD 5200.28-STD, December 1985.

Sections 2.1.2.1, 2.2.2.1, 3.1.2.1, 3.2.2.1, 3.3.2.1, and 4.1.2.1 contain the I&A requirements, which are summarized on page 101. Sections 3.2.2.1.1, 3.3.2.1.1, and 4.1.2.1.1 contain the trusted path requirements, which are summarized on pages 107-108.

INTERP94 National Computer Security Center, *The Interpreted TCSEC Requirements*, (quarterly).

The following Interpretations are relevant to I&A:

I-0001	Delayed enforcement of authorization change
I-0096	Blanking passwords
I-0240	Passwords may be used for card input
I-0288	Actions allowed before I&A
C1-CI-02-83	Identification and Authentication
C1-CI-02-86	Server
C1-CI-04-86	Operator Log-on (supersedes C1-CI-02-83)

The following Interpretation is relevant to trusted path:

C1-CI-01-86	Discretionary Access Control

Gasser88 Gasser, M., *Building a Secure Computer System*, Van Nostrand Reinhold Co., N.Y., 1988.

Section 3.3.2 presents an introduction to I&A. Section 6.1 talks about passwords and protecting authentication data. Section 10.4 talks about trusted path.

PASS85 National Computer Security Center, *Department of Defense Password Management Guideline*, CSC-STD-002-85, April 1985.

This document provides guidelines on the use of password-based user authentication mechanisms in trusted systems. Describes good practices related to assigning passwords (machine generation), maintaining passwords (ISSO and user responsibilities), and authentication mechanism functionality.

I&A91 National Computer Security Center, *A Guide to Understanding Identification and Authentication in Trusted Systems*, NCSC-TG-017, Version 1, September 1991.

This document provides guidance to vendors on how to design and incorporate effective I&A mechanisms into their systems. Also helps vendors and evaluators understand I&A requirements for classes C1 through A1 of the TCSEC. Discusses the purpose of I&A, how I&A works, what are the typical aspects of effective authentication, the importance of securing authentication data, and describes some possible methods of implementation.

Wood77 Wood, H., "The Use of Passwords for Controlling Access to Remote Computer Systems and Services," *Proceedings of the 7th National Computer Conference*, pp. 27-33, 1977.

This early paper presents many of the concerns addressed in subsequent research on personal authentication methods. The

three authentication approaches are introduced, and arguments made that the password approach is the most economical and likely to be used approach. Methods to improve the resistance of password-based systems to penetration are discussed.

Carlton88 Carlton, S.F., Taylor, J.W., and Wyszynski, J.L., "Alternate Authentication Mechanisms," *Proceedings of the 11th National Computer Security Conference*, pp. 333-338, October 1988.

This paper provides a more current and in-depth analysis of the strengths and weaknesses of the three authentication approaches: (1) something you know (e.g., passwords),(2) something you possess (e.g., smart card), and (3) somethingyou are (e.g., retinal scanner). Representative commercial authentication products are discussed.

Supplemental Readings

PFX86 National Computer Security Center, *Final Evaluation Report of Sytek PFX A2000 and PFX A2100*, CSC-EPL-86/006, 7 November 1986. (Note: These devices are now owned and marketed by RACAL-GUARDATA).

This report presents NCSC's evaluation of the authentication device described in [Wong85]. This document is included mainly as an example of an evaluation report; the design detail of the product is less important.

Troy86 Troy, E.F., "Limitations of Dial-Up Security Devices," *Proceedings of the 9th National Computer Security Conference*, pp. 62-70, September 1986.

This paper reviews the I&A advantages offered by dial-up devices, describes their basic characteristics through examples, and discusses their weaknesses (economic, practical, and security related). Dial-up devices are separated into six major groups according to their primary protection objective: host port protection devices, user terminal security modems, user authentication devices, terminal identification devices, line encryption devices, and message authentication devices.

Other Readings

ACES87 National Computer Security Center, *Final Evaluation Report of Security Dynamics Access Control Encryption System*, CSC-EPL-87/001, 31 March 1987.

AK86 National Computer Security Center, *Final Evaluation Report of Gordian Systems Access Key*, CSC-EPL-86/001, 7 April 1986.

Berson88 Berson, T., Capek, P., Schweitzer, J., and Weissman, C., "Identity Verification (Authentication) Working Group -- Final Report, January 1988," *SIGSAC (Security Audit & Control) Review*, Vol. 6, No. 1, pp. 2-9. ACM, New York, NY, Spring 1988.

Botting86 Botting, R., "Novel Security Techniques for On-Line Systems," *Communications of the ACM*, Vol. 29, No. 5, pp. 416-417, May 1986.

CPP86 National Computer Security Center, *Final Evaluation Report of Codercard Cpp-300 Port Protector*, CSC-EPL-86/002, 7 April 1986.

IDX88 National Computer Security Center, *Final Evaluation Report of Identix, Inc. IDX-50*, CSC-EPL-88/001, 1 February 1988.

Murray84 Murray, W., "Good Computer Security Practices for Two Areas of Current Concern: Personal Computers and Dial-up Systems," *Advances In Computer System Security*, Vol. II, 1984.

Morris79 Morris, R. and Thompson, K., "UNIX Password Security: A Case History," *Communications of the ACM*, Vol 22, No. 11, November 1979.

Spender86 Spender, J-C., "Computer Security and User Authentication: Old Problems, New Solutions," *AIAA/ASIS/DODCI Second Aerospace Computer Security Conference*, pp. 126-132, December 1986.

Wisema88 Wiseman, S., Terry, P., Wood, A., and Harrold, C., "The Trusted Path between SMITE and the User," *Proceedings of the 1988 IEEE Symposium on Security and Privacy*, pp. 147-155, April 1988.

Wong85 Wong, R., Berson, T., Feiertag, R., "Polonius: An Identity Authentication System," *Proceedings of the 1985 IEEE Symposium on Security and Privacy*, pp. 101-107, April 1985.